BUREAU RESPONSE TO A BREACH OF CONFIDENTIAL INFORMATION

PURPOSE

This policy describes the action required of the Texas Department of Health (TDH), Bureau of HIV and STD Prevention (Bureau) in the event that confidential client information it retains is released either accidentally or intentionally. The policy also discusses the procedure the Bureau will use when it becomes aware of a suspected breach of confidential information by an entity with which it is associated either contractually or professionally.

BACKGROUND

The Bureau obtains certain personal and private information from the individuals they serve by virtue of fulfilling its mission to prevent, treat and control the spread of HIV, STDs and other communicable diseases. These individuals trust that the Bureau will take every precaution to protect that information in order to retain their confidentiality. The Bureau must be vigilant in maintaining the integrity of systems that contain the information. Potential breaches may come in the form of insiders who make innocent mistakes and cause accidental disclosures; insiders who abuse access privileges; insiders and outsiders who knowingly access information for spite or profit; an unauthorized physical intruder, and vengeful employees and outsiders who attempt to access information to damage systems and disrupt operations. The Bureau must respond to any breach of confidential information in a rapid and decisive manner to mitigate the effects of such a release and prevent any recurrence of a similar incident. The Bureau may also become aware of a suspected breach of confidential information by an organization with which it has a contractual agreement or a health care professional involved in HIV and STD diagnosis, treatment or prevention. In this situation, the Bureau has an obligation to the public to intervene, to the extent possible, on behalf of those affected.

AUTHORITY

V.T.C.A., Penal Code, Chapter 16, Chapter 33; V.T.C.A, Health and Safety Code, §81.046 and 81.103; V.T.C.A.; Texas Government Code, Chapter 552.

DEFINITIONS

Breach of confidentiality an incident in which confidential client information is known to have been: 1. accidentally or intentionally released verbally, electronically or by paper media to an entity which by law does not

	have a right or need to know or 2. purposefully accessed with an intent to cause damage.
Confidential client information	demographic and/or clinical information deemed to be confidential by law which pertains to a client that could result in the identification of the client should that information be released by any method.
Personnel action	adverse action that may be taken against a Bureau employee who causes a breach in confidentiality.
Risk analysis	a process by which reasonable and cost effective security control measures are selected as measured against any expected losses if those measures were absent.
Security plan	the framework within which an organization establishes needed levels of information security to achieve its desired confidentiality goals.

APPLICABILITY

This policy applies to all Bureau employees, temporary employees, volunteers, students, and its agents. Bureau staff may share this policy as a model for contractors who must establish confidentiality policies for the confidential information maintained by their own agencies.

POLICIES RELATED TO BUREAU SECURITY AND CONFIDENTIALITY

The following policies enable the Bureau's basic security plan: HIV/STD Policy Definitions; HIV/STD Policy No. 020.004, *Confidentiality, Bureau Employees*; HIV/STD Policy No. 020.005, *Retention and Storage of HIV and STD Client Data Records*; HIV/STD Policy No. 020.008, *Public Information Request, Handling Under the Public Information Act*; HIV/STD Policy No. 020.041, *Security*; HIV/STD Policy No. 020.050, *Public Complaints and Allegations Related to the Delivery of HIV or STD Programs*; HIV/STD Policy No. 020.060, *Publication or Release of HIV/STD Data*; HIV/STD Policy No. 040.001, *Confidential Information, Handling and Transmission*; HIV/STD Policy No. 044.001, *Computer Equipment and Software, Personal Use of*; HIV/STD Policy No. 044.011, *Use of the Internet*; HIV/STD Policy No. 530.001, *Reporting Suspected Abuse and Neglect of Children*; HIV/STD Policy No. 550.001, *Transmission of Confidential Medical Information, Requirements for Contractors*; HIV/STD Policy No. 700.003, *HIV/STD Medication Program, Pharmacy Eligibility Criteria*. Additional policies may be added should the need arise. All persons to whom this policy is applicable must be familiar with the relevant policies and the data security practices of the Bureau.

METHODS OF PREVENTING COMMON BREACHES OF CONFIDENTIALITY

Listed below are facets of information security that may not be specifically mentioned in the policies listed but are preventative in nature and ongoing.

Personnel related issues

- Inform departing employees having had access to confidential client information that they are still under obligation to retain confidentiality
- Insure that user access to computer and physical facilities is removed when leaving employment for any reason. See Bureau Policy No. 020.041
- Provide security awareness training on computer use
- Provide user education in password management
- Provide periodic security reminders

Continuing office practices

- Insure that staff are trained in the methods used to fax confidential information
- Review filing procedures for hard copies of confidential information
- Conduct desk reviews to determine if staff are correctly securing confidential information

Providing for physical safeguards to maintain data integrity, confidentiality and availability

- Review plans to protect resources from fire and other natural and/or environmental hazards
- Review and revise the facility security plan
- Update and review technical security mechanisms which guard against unauthorized access to data that is transmitted over the communications network

RESPONSIBILITY FOR INVESTIGATING A RELEASE OF CONFIDENTIAL INFORMATION

The Bureau security team is responsible for investigating any suspected unauthorized access or release of confidential information. This team consists of the Bureau Chief, the Staff Services Officer, and the Information Systems Branch Manager.

In the event an internal breach of confidentiality is suspected, the Division Director of the program area in which the breach may have occurred is added to the team.

INITIAL ACTION IN RESPONSE TO A REPORTED BREACH OF CONFIDENTIALITY

Suspected breach by an entity outside of TDH is reported by an external source

Reports of a breach of confidentiality from a source outside the Bureau are handled as an immediate threat to clients as outlined in HIV/STD Policy No. 020.050, *Public Complaints and Allegations Related to the Delivery of HIV or STD Programs*. Staff receiving the report of the breach must immediately refer the incident to a member of the Bureau's Complaint Triage Committee or the Bureau security team.

The external person who reports the breach, whether that person is the affected client or not, must be given the option of remaining anonymous.

Reports received by the complaint triage committee are to be referred to the Bureau security team for investigation and resolution. Staff receiving the report of the breach must follow up immediately by completing a Complaint Intake Form (211.001a) for the particular incident and hand-delivering the report to a member of the Bureau security team. The report must outline the known details of the incident including, if possible, the name of the party affected by the suspected breach, the sequence of events leading to the release, when and where it happened, what action was taken and by whom.

The procedure outlined in Bureau procedure BUR-BCO-211.001 will govern the investigation process of the suspected breach. However, the Bureau security team may diverge from the procedure as may be necessary to conduct a complete investigation in the most timely manner possible.

Internal breach is discovered and reported by Bureau staff

The staff member discovering an actual or potential breach of confidentiality must take whatever immediate steps are necessary to prevent any additional loss of data. It may be necessary to ensure that doors and files are shut and locked as necessary or to report unauthorized persons in the building. The staff person must notify the most immediate supervisory staff available about the breach.

Any employee who caused the breach, and may continue to pose a security risk, must be treated as an immediate threat to Bureau security. All of the employee's access to Bureau physical and electronic resources must be limited or rescinded until an investigation of the incident is complete. Options on handling the situation include: immediately reassigning the employee to a temporary duty station; obtaining permission from the Bureau Chief, the Staff Services Officer or the director of the division to which the employee is assigned, to send the employee home pending investigation of the breach, or calling law enforcement personnel in extreme situations.

Once the immediate problem is resolved or stabilized the Bureau will respond in the following manner:

- Within 24 hours of the discovery of a loss of a client record or release of confidential information, staff shall complete a written security incident report for the particular incident using Complaint Intake Form, 211-001a (available under S:\FORMS\211-001a.frm or Windows Group Forms). The report must outline details of the incident, the sequence of events leading to the release, when and where it happened, what action was taken and by whom.
- The completed and signed report is routed to the Bureau security team for triage.

INVESTIGATIVE STAGE OF ACTION IN RESPONSE TO A REPORTED BREACH OF CONFIDENTIALITY

The Bureau security team provides organizational focus and importance on security by determining the validity of a suspected breach of confidentiality.

When the reported breach is found to be invalid, the Bureau security team ensures that the person who reported the suspected breach is notified of the findings and closes out the complaint report.

Upon finding an actual breach of confidentiality and ascertaining the scope of the breach, the Bureau security team directs the Bureau's internal and external response by utilizing any combination of the following actions:

- informing, in this order, the Office of General Counsel, the Associate Commissioner for Disease Control and Prevention, the Deputy Commissioner for Public Health Sciences and Quality, the Commissioner of Health, Public Health Promotion Program and other appropriate senior departmental staff if appropriate;
- notifying appropriate licensure authorities when the complaint is related to an agency or individual regulated by a licensing authority;
- referring the complaint to a Contractor whose staff may have caused the breach and following up on the resolution of the complaint;
- reviewing the circumstances surrounding the breach of confidentiality;
- conducting a risk analysis;
- implementing new or additional processes to address any deficiencies in the Bureau's security plan;
- determining what personnel actions are to be imposed on the individual(s) responsible for the breach (Refer to HIV/STD Policy No. 020.004);
- applying sanctions to a Contractor that does not take prompt action to resolve the complaint (Refer to HIV/STD Policy No. 540.001);
- directing staff who accepted the reported breach to contact the affected client(s) to determine the extent of any harm done and provide information about the action(s) being taken in regard to the breach, and
- pursuing legal remedy against an individual or Contractor found to be responsible for releasing confidential information.

Bureau security team review areas

The Bureau security review team will consider all or part of the security management processes including accountability, management controls, electronic controls, physical security controls and penalties for the abuse and misuse of the Bureau's physical and electronic assets.

MEDIA CONTACTS

All media contacts related to a breach of confidentiality are to be handled in accordance with Bureau Procedure, BUR-BCO-211.005.

RECORD RETENTION

All incident reports will be entered in BATS and stored along with all associated documentation in a central file after resolution. These records will be retained according to the State of Texas Record Retention Schedule, 502 - Bureau of HIV and STD Prevention, under the record series title relating to complaints.

DATE OF LAST REVIEW:
November 13, 2002 Converted format from WordPerfect to Word.

REVISIONS

Page 3, line 12 Deleted "or Section Chief"